REMARKS

Claims 1, 3, 5, 7, and 10 have been amended to merely clarify the invention. No new matter is introduced by the amendments of these claims. Claims 1-11 remain pending.

The Examiner has indicated that claims 3 and 4 would be allowable if amended to overcome the 35 U.S.C. §112, 2nd paragraph, rejection. However, since there is no outstanding rejection with respect to claims 3 and 4 in the Office Action of 13 May 2008, it is presumed that the Examiner meant that these claims are allowable.

The Examiner has rejected claims 1 and 2 under 35 U.S.C. §103(a), as being unpatentable over Fijolek et al. (U.S. Patent 6,510,162) in view of Fijolek et al. (US Patent 6,577,642) and in further view of Casey (US Patent 6,493,349). Additionally, claims 5 and 6 are rejected under 35 U.S.C. §103(a) as being unpatentable over Fijolek et al. in view of Rosen et al. ("BGP/MPLS VPN's" 1999) and Casey. Claims 7-9 are rejected under 35 U.S.C. §103(a) as being unpatentable over Fijolek et al. in view of Rosen and Casey and further in view of Gilbrech (US patent 6,173,399). Claims 10 and 11 are rejected under 35 U.S.C. §103(a) as being unpatentable over Fijolek et al. in view of Casey and Rosen. The Examiner's rejections are respectfully traversed as follows.

Claim 1 is directed towards an "apparatus for routing packets from a first network node to a second network node in a data network." Claim 1 also recites "means for assigning and then sending a unique first node identifier (ID) to the first node, wherein the unique first node ID uniquely identifies the first node" and "means for mapping the assigned unique first node ID with at least one VPN, wherein the unique first node ID is assigned, sent, and mapped by an entity other than the first node." Claim 1 also requires "means for receiving a packet from the first node, said packet including the unique first node ID, and including routing information for routing said packet to a destination address associated with said second node" and "means for examining the packet to identify the first node ID of the first node." Claim 1 further requires "means for using said unique first node ID, routing information, and the mapping between the unique first node ID and the at least one VPN to determine whether said first node is associated with at least one VPN." Claim 5 recites "means for if it is determined that said first node is a member of at least one VPN, assigning and then sending a unique identifier (ID) to the first node and binding the unique ID of said first node with said VPN to thereby cause said first node to be associated with said VPN, wherein the unique ID is assigned, sent, and then bound by an entity other than the first node, wherein the unique ID uniquely identifies the first node." Claim 10 recites "means for assigning and then sending to the first node a unique identifier (ID), wherein the unique ID is assigned and sent to the first node by an entity other than the first node, wherein

the unique ID uniquely identifies the first node" and "means for associating the assigned unique ID with the first VPN to thereby cause the first node to be associated with the first VPN, wherein the assigned unique ID is associated by the entity other than the first node."

Embodiments of the present invention include mechanisms for assigning a unique ID to a node and then sending such unique ID to the node, wherein the unique ID is assigned and sent by an entity other than the node. This assigned and sent unique ID is also mapped or associated with one or more VPN's by such other entity or device. Thus, when a packet having the assigned unique ID is received by such other device from the node that received such unique ID, this other device may determine whether the node belongs to a particular VPN based on the returned, unique ID and the mapping or associating of such unique ID. Accordingly, the node does not have to utilize a VPN label or implement any kind of VPN protocol in order to take advantage of a VPN arrangement since an intermediary device can determine the VPN of the node based on the assigned unique ID and mapping of such unique ID to a particular VPN.

Although the primary reference Fijolek discloses assigning a unique identifier in the form of an service identifier or SID, Fijolek fails to disclose "means for mapping the assigned unique ID with at least one VPN" or "means for using said unique first node ID, routing information, and the mapping between the unique first node ID and the at least one VPN to determine whether said first node is associated with at least one VPN" of claim 1. Likewise, Fijolek fails to disclose "means for... binding the unique ID of said first node with said VPN to thereby cause said first node to be associated with said VPN" of claim 5 or "means for associating the assigned unique ID with the first VPN to thereby cause the first node to be associated with the first VPN" of claim 10.

The secondary references also fail to teach these features. For instance, it is respectfully submitted that the secondary reference Casey is directed towards utilizing a standard VPN protocol to determine the VPN of a particular node. Although Casey teaches providing a VPN ID for a node, it is submitted that Casey fails to teach mechanisms for mapping, binding, or associating a unique ID with a VPN, in the manner claimed. Casey also fails teach mechanisms for utilizing such mapping, binding, or association between such unique ID and VPN to determine whether the node (with the assigned unique ID) is associated with one or more VPN's, in the manner claimed. In contrast, Casey discloses associating a non-unique VPN identifier with multiple nodes and utilizing such non-unique association for VPN determination. See Col. 2, Lines 16-19 (Emphasis added): "VPN identifier assigned to the first router is the same as the VPN identifier assigned to the second router." This infrastructure "enables private communications over shared network, between at least two geographically separate private networks." See Col. 2, Lines 4-6. That is, non-unique VPN identifiers are assigned to different

routers so that such different routers can utilize a same VPN. Since Casey discloses using non-unique VPN identifiers for VPN mapping and determination, Casey fails to teach or suggest mapping, binding, associating a unique ID to a specific VPN, in the manner claimed. Additionally, Casey also necessarily fails to teach or suggest the use of such a mapping, binding, or association between a unique ID and a VPN, in the manner claimed. The secondary references Gilbrech and Rosen also fail teach or suggest such limitations.

The Examiner's rejections of the dependent claims are also respectfully traversed. However, to expedite prosecution, all of these claims will not be argued separately. Claims 2, 6-9, and 11 each depend directly or indirectly from independent claims 1, 5, or 10 and, therefore, are respectfully submitted to be patentable over cited art for at least the reasons set forth above with respect to claims 1, 5, or 10. Further, the dependent claims require additional elements that when considered in context of the claimed inventions further patentably distinguish the invention from the cited art.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. If the Examiner believes that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number listed at the bottom of this page.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Mary R. Olynick/

Mary R. Olynick
Reg. 42,963

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100